Note Méthodologique : Commandes et Automatismes en Sécurité des Équipements

Synthèse structurée de la démarche et des étapes de réalisation de la mission.

> **Point clé :** La robustesse repose sur l'allocation d'exigences (PL/SIL), une architecture lisible, une validation indépendante et une discipline d'exploitation (essais périodiques, gestion des changements).

Contexte & finalité de la méthodologie

- Modernisation des machines → fonctions de commande plus sophistiquées et risques accrus.
- Objectif: prévenir défaillances de conception, d'usage et de maintenance.
- Approche intégrée: sécurité fonctionnelle, ergonomie IHM, gestion du cycle de vie.
- Piliers: analyse des risques, catégorisation des fonctions, choix d'architectures, contrôle des modifications.
- Levier de performance: réduction arrêts intempestifs, quasi-accidents et coûts cachés.

Objectifs de la mission

- Atteindre un niveau cible PL d ou SIL 2 pour les fonctions critiques.
- Assurer un temps de réaction compatible avec la distance de sécurité.
- Documenter les preuves de validation et d'essais périodiques.
- Gérer les changements via un processus formalisé et tracé.
- Garantir la disponibilité de la fonction d'arrêt d'urgence à tous les postes.

Périmètre / livrables attendus

- Matrice de risques et hypothèses d'architecture (cadrage, modes de marche et limites d'utilisation).
- Choix d'architectures et schémas formalisés (fonctions d'arrêt, interverrouillages, capteurs/actionneurs).
- Plan de tests, critères d'acceptation, essais y compris négatifs, mesures de temps de réaction.
- Dossier de preuves et documentation consolidée (validation, diagnostics, résultats d'essais).
- Revue d'acceptation en mise en service et plan de surveillance initial.
- Registre des fonctions de sécurité, calendrier d'essais périodiques et processus de gestion des modifications.
- Rituel de revue (mensuel/trimestriel) et indicateurs de performance sécurité.

Démarche méthodologique (étapes)

1) Cadrage & analyse des risques

- Cartographier dangers, modes de marche, limites d'utilisation; intégrer REX incidents/quasi-accidents.
- Allouer fonctions de sécurité cibles et niveaux d'intégrité attendus.
- Livrables: matrice de risque, premières hypothèses d'architecture.

2) Conception d'architectures & choix technologiques

- Structurer fonctions (arrêts, commandes, interverrouillages); dimensionner capteurs/actionneurs.
- Arbitrer relais de sécurité vs automates de sécurité; principes de redondance/diagnostic.
- Livrables: schémas formalisés et architecture compatible exploitation/maintenance.

3) Programmation, vérification & validation fonctionnelle

- Plan de tests (modes, défauts, pertes d'énergie); critères d'acceptation; traçabilité.
- Essais négatifs, mesure des temps de réaction; séparation sécurité/automatisme standard.
- Livrables: résultats d'essais et dossier de preuve de conformité.

4) Mise en service, formation & transfert

- Vérification en conditions réelles; revue d'acceptation avec parties prenantes.
- Formation opérateurs/mainteneurs (modes, réarmement, conduite en mode dégradé autorisé).
- Livrables: documentation consolidée; plan de surveillance initial (quelques semaines).

5) Exploitation, essais périodiques & gestion des changements

- Structurer registre des fonctions, calendrier d'essais périodiques, processus de modifications.
- Planifier, exécuter et consigner tests; analyser défauts; décider actions correctives.
- Livrables: traçabilité complète et revalidation selon le risque.

6) Retour d'expérience & amélioration continue

- Analyser incidents, arrêts intempestifs, quasi-accidents (technique et humain).
- Mettre à jour schémas, paramètres, procédures; décider sur indicateurs cibles.
- Rituel de revue mensuel ou trimestriel avec décisions tracées.

Planning / durée / jalons

Phase	Jalons / sorties	Durée / notes
1) Cadrage & risques	Matrice de risques validée; hypothèses d'architecture; REX intégré	—
2) Conception archi	Schémas préliminaires; choix relais/automate; principes de redondance	—
3) Prog & validation	Plan de tests; essais négatifs; mesures temps de réaction; dossier de preuves	Vérification indépendante
4) Mise en service	Revue d'acceptation; documentation finalisée; formation	Surveillance initiale: quelques semaines

5) Exploitation	Registre des fonctions; calendrier d’essais; processus de changements	Traçabilité et revalidation selon risque
6) Amélioration	Revue mensuelle / trimestrielle; indicateurs; décisions tracées	Boucle continue

Rôles & responsabilités

Client

- Fournir l’inventaire des modes de marche et le REX (incidents, quasi-accidents).
- Participer à l’analyse des risques et valider la matrice et les hypothèses d’architecture.
- Réaliser/planifier les essais périodiques, consigner résultats et écarts.
- Maintenir la documentation à jour; assurer gouvernance des accès/versions.
- Former et impliquer opérateurs/maintenance dans l’exploitation (réarmement, modes).

Consultant

- Conduire le diagnostic; structurer l’analyse des risques et l’allocation PL/SIL.
- Appuyer le choix d’architectures et la formalisation des schémas.
- Définir le plan de tests; piloter la vérification/validation indépendante.
- Animer la revue d’acceptation; outiller registre et calendrier d’essais.
- Accompagner la gestion des changements et la montée en compétences.

Prérequis & données nécessaires (inputs)

- Vision partagée des dangers, modes (automatique, réglage, nettoyage, essais) et limites d’utilisation.
- Retours d’expérience (incidents, quasi-accidents) et contextes d’intervention.
- Exigences d’intégrité visées (PL/SIL) et référentiels applicables.
- Données de distances/temps (compatibilité ISO 13855) et scénarios transitoires (réarmement, basculement de mode).
- Inventaire capteurs/actionneurs, interfaces systèmes et contraintes CEM.
- Schémas existants, versions logicielles, politique d’accès/sauvegarde.
- Critères de tests et formats attendus pour la traçabilité des preuves.

Modalités de pilotage & qualité (comités, validations, risques)

- Validation/vérification indépendante; séparation claire sécurité vs automatisme standard.
- Processus formalisé de gestion des changements (description, analyse d’impact, tests, revalidation).
- Plan d’essais périodiques basé sur la criticité; tests négatifs; mesures des temps de réaction.
- Traçabilité: journaux d’événements, registre des fonctions, résultats d’essais et actions correctives.
- Rituel de revue mensuel/trimestriel avec indicateurs et décisions tracées.

- Indicateurs: conformité essais planifiés/réalisés, temps moyen de réarmement, taux d’arrêts intempestifs, anomalies de diagnostic, délais de mise à jour documentaire.
- Focus risques: états transitoires mal couverts, interfaces hétérogènes, complexité inutile, dette de maintenance logicielle.
